УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 151, кн. 2 Физико-математические науки *2009*

УДК 519.7

БЫСТРЫЙ АЛГОРИТМ ПОСТРОЕНИЯ ВЕКТОРОВ КОЭФФИЦИЕНТОВ ПОЛЯРИЗОВАННЫХ ПОЛИНОМОВ k-ЗНАЧНЫХ ФУНКЦИЙ

С.Н. Селезнева, Н.К. Маркелов

Аннотация

Предложен быстрый алгоритм построения векторов коэффициентов поляризованных полиномов k-значных функций по векторам их значений (при простых k). Получены формулы подсчета по значениям k-значных функций коэффициентов их поляризованных полиномов.

Ключевые слова: k-значная функция, поляризованный полином, быстрый алгоритм.

Одним из способов задания k-значных функций являются полиномы. Обычные и поляризованные полиномы являются каноническими формами записи функций [1, 2].

Известны быстрые алгоритмы нахождения векторов коэффициентов обычных и поляризованных полиномов булевых функций по векторам их значений [3, 4]. Ю.В. Таранниковым[1] предложен быстрый алгоритм нахождения вектора коэффициентов обычных полиномов k-значных функций (при простых $k \geq 3$) по векторам их значений. В настоящей статье нами предложен аналогичный быстрый алгоритм нахождения векторов коэффициентов поляризованных полиномов k-значных функций (при простых $k \geq 3$) по векторам их значений.

Кроме того, нами найдены явные формулы подсчета значений коэффициентов поляризованных полиномов k-значных функций по их значениям. Для булевых функций формулы подсчета значений коэффициентов обычных полиномов можно найти в [5].

Пусть $k \geq 2$, $E_k = \{0, 1, \ldots, k-1\}$. Назовем k-значной функцией отображение $f^n : E_k^n \to E_k$, $n = 0, 1, \ldots$ Множество всех k-значных функций обозначим как P_k, множество всех k-значных функций, зависящих от переменных $x_1, \ldots, x_n$, обозначим как P_k^n.

Будем рассматривать сложение и умножение по $\bmod k$.

Пусть $\delta = (d_1, \ldots, d_n) \in E_k^n$. *Поляризованным полиномом по вектору поляризации* δ назовем полином

$$\sum_{\alpha=(a_1,\ldots,a_n)\in E_k^n} c_f^\delta(\alpha)\,(x_1 + d_1)^{a_1} \cdots (x_n + d_n)^{a_n},$$

в котором $c_f^\delta(\alpha) \in E_k$ – некоторые коэффициенты и $(x_i + d_i)^{a_i}$ – степени, то есть

$$(x_i + d_i)^{a_i} = \underbrace{(x_i + d_i)\,(x_i + d_i) \cdots (x_i + d_i)}_{a_i \text{ раз}}, \quad (x_i + d_i)^0 = 1.$$

[1] Личное сообщение.

Если $\delta = (0, \ldots, 0)$, то поляризованный по вектору δ полином – обычный полином по mod k. В этом случае в коэффициентах будем опускать верхний индекс δ.

Если k – простое число, то каждая функция $f(\tilde{x}^n) \in P_k^n$ однозначно задается полиномом по mod k [1], и для каждой функции $f(\tilde{x}^n) \in P_k^n$ существует единственный полином, поляризованный по произвольному вектору δ из E_k^n [2] .

Далее будем полагать, что k – простое число.

Назовем *вектором коэффициентов* поляризованного по вектору поляризации $\delta \in E_k^n$ полинома функции $f(\tilde{x}^n) \in P_k^n$ вектор значений функции $c_f^\delta(\tilde{x}^n)$.

Известен быстрый алгоритм построения вектора коэффициентов полинома Жегалкина булевых функций [3]. В.П. Супруном [4] найден быстрый алгоритм построения векторов коэффициентов поляризованных полиномов булевых функций. Ю.В. Таранниковым[2] был найден быстрый алгоритм построения вектора коэффициентов обычного полинома для k-значных функций.

В следующей теореме 1 мы предлагаем аналогичный быстрый алгоритм вычисления вектора коэффициентов поляризованных полиномов k-значных функций.

Теорема 1. *Пусть k – простое число, $f(\tilde{x}^n) \in P_k^n$, $f_i(x_2, \ldots, x_n) = f(i, x_2, \ldots, x_n)$, $i \in E_k$, $\delta = (d_1, \ldots, d_n)$ и $\delta' = (d_2, \ldots, d_n)$.*

Тогда если $n = 1$, то

$$c_f^\delta(0) = f(-d_1),$$
$$c_f^\delta(j) = -\sum_{i=1}^{k-1} i^{(k-1)-j} f(i - d_1), \quad \textit{если} \quad j = 1, \ldots, k-2,$$
$$c_f^\delta(k-1) = -\sum_{i=0}^{k-1} f(i - d_1),$$

и при $n \geq 2$

$$c_f^\delta(0, x_2, \ldots, x_n) = c_{f_{-d_1}}^{\delta'}(x_2, \ldots, x_n),$$
$$c_f^\delta(j, x_2, \ldots, x_n) = -\sum_{i=1}^{k-1} i^{(k-1)-j} c_{f_{j-d_1}}^{\delta'}(x_2, \ldots, x_n), \quad \textit{если} \quad j = 1, \ldots, k-2,$$
$$c_f^\delta(k-1, x_2, \ldots, x_n) = -\sum_{i=0}^{k-1} c_{f_{i-d_1}}^{\delta'}(x_2, \ldots, x_n),$$

где сумма векторов берется покоординатно.

Доказательство. Вначале докажем вспомогательное утверждение.

Лемма 1. *Для каждого простого числа k*

$$\sum_{i=1}^{k-1} i^s = \begin{cases} k-1, & s = k-1, \\ 0, & s = 1, \ldots, k-2. \end{cases}$$

Доказательство. Если $s = k-1$, то $\sum\limits_{i=1}^{k-1} i^{k-1} = k-1$ по малой теореме Ферма.

Для $s = 1, \ldots, k-2$ проведем доказательство индукцией по значению s.

Базис индукции. Если $s = 1$, то $\sum\limits_{i=1}^{k-1} i = \dfrac{k(k-1)}{2} = 0$ ввиду простоты k.

[2]Личное сообщение.

Индуктивный переход. Допустим, что лемма верна для всех s, $s = 1, \ldots, m-1 < k-2$. Проверим ее справедливость для $s = m$.

С учетом индуктивного предположения получаем

$$0 = k^{m+1} = \sum_{i=0}^{k-1}((i+1)^{m+1} - i^{m+1}) = \sum_{i=0}^{k-1}\sum_{j=1}^{m+1} C_{m+1}^{j} i^{m+1-j} =$$

$$= \sum_{j=1}^{m+1} C_{m+1}^{j} \sum_{i=0}^{k-1} i^{m+1-j} = (m+1)\sum_{i=0}^{k-1} i^{m}.$$

Так как $m+1 \neq 0$, то

$$\sum_{i=0}^{k-1} i^{m} = 0.$$

Лемма 1 доказана. □

Теперь докажем теорему.

1. Вначале рассмотрим обычные полиномы, то есть предположим, что вектор поляризации $\delta = (0, \ldots, 0)$. Доказательство этого пункта отлично от обоснования алгоритма Ю.В. Таранникова для обычных полиномов.

Пусть

$$f(x_1, x_2, \ldots, x_n) = x_1^{k-1} g_{k-1}(x_2, \ldots, x_n) + \cdots + x_1 g_1(x_2, \ldots, x_n) + g_0(x_2, \ldots, x_n),$$

где $g_{k-1}, \ldots, g_1, g_0$ – полиномы от переменных $x_2, \ldots, x_n$ (или константы, если $n = 1$).

Несложно заметить, что $g_0(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n)$.

С учетом леммы 1 и полагая, что $0^0 = 1$, получаем

$$\sum_{i=0}^{k-1} f(i, x_2, \ldots, x_n) = \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} i^j g_j(x_2, \ldots, x_n) =$$

$$= \sum_{j=0}^{k-1} g_j(x_2, \ldots, x_n) \sum_{i=0}^{k-1} i^j = (k-1) g_{k-1}(x_2, \ldots, x_n).$$

Откуда, $g_{k-1}(x_2, \ldots, x_n) = -\sum\limits_{i=0}^{k-1} f(i, x_2, \ldots, x_n)$.

Пусть теперь $1 \leq j \leq k-2$. Рассмотрим функцию

$$h(x_1, \ldots, x_n) = x_1^{(k-1)-j} f(x_1, \ldots, x_n) =$$

$$= x_1^{k-1} g'_{k-1}(x_2, \ldots, x_n) + \cdots + x_1 g'_1(x_2, \ldots, x_n) + g'_0(x_2, \ldots, x_n),$$

где $g'_{k-1}, \ldots, g'_1, g'_0$ – полиномы от переменных $x_2, \ldots, x_n$ (или константы, если $n = 1$).

Заметим, что $g'_{k-1}(x_2, \ldots, x_n) = g_j(x_2, \ldots, x_n)$. По уже доказанному

$$g'_{k-1}(x_2, \ldots, x_n) = -\sum_{i=0}^{k-1} g(i, x_2, \ldots, x_n) = -\sum_{i=0}^{k-1} i^{(k-1)-j} f(i, x_2, \ldots, x_n),$$

откуда $g_j(x_2, \ldots, x_n) = -\sum\limits_{i=1}^{k-1} i^{(k-1)-j} f(i, x_2, \ldots, x_n)$, $j = 1, \ldots, k-2$.

Теперь пусть $n = 1$. Тогда каждая из функций $g_{k-1}, \dots, g_1, g_0$ является константой и $c_f(j) = g_j$, $j = k-1, \dots, 1, 0$.

Тогда по доказанному

$$c_f(0) = f(0);$$

$$c_f(j) = -\sum_{i=1}^{k-1} i^{k-1-j} f(i),\ j = 1, \dots, k-2;$$

$$c_f(k-1) = -\sum_{i=0}^{k-1} f(i).$$

Если $n \geq 2$, то $c_f(j, x_2, \dots, x_n) = c_{g_j}(x_2, \dots, x_n)$. Откуда по доказанному

$$c_f(0, x_2, \dots, x_n) = c_{f_0}(x_2, \dots, x_n);$$

$$c_f(j, x_2, \dots, x_n) = -\sum_{i=1}^{k-1} i^{k-1-j} c_{f_i}(x_2, \dots, x_n),\ j = 1, \dots, k-2;$$

$$c_f(k-1, x_2, \dots, x_n) = -\sum_{i=0}^{k-1} c_{f_i}(x_2, \dots, x_n).$$

2. Теперь рассмотрим произвольный вектор поляризации $\delta = (d_1, \dots, d_n)$. Воспользуемся тем, что поляризованный по вектору $\delta = (d_1, \dots, d_n)$ полином функции $f(x_1, \dots, x_n)$ является обычным полиномом для функции

$$g(x_1, \dots, x_n) = f(x_1 - d_1, \dots, x_n - d_n).$$

Тогда при $n = 1$

$$c_f^\delta(0) = c_g(0) = g(0) = f(-d_1);$$

$$c_f^\delta(j) = c_g(j) = -\sum_{i=1}^{k-1} i^{k-1-j} g(i) = -\sum_{i=1}^{k-1} i^{k-1-j} f(i - d_1), \quad j = 1, \dots, k-2;$$

$$c_f^\delta(k-1) = c_g(k-1) = -\sum_{i=0}^{k-1} g(i) = -\sum_{i=0}^{k-1} f(i - d_1).$$

При $n \geq 2$ положим $\delta' = (d_2, \dots, d_n)$. Тогда

$$c_f^\delta(0, x_2, \dots, x_n) = c_g(0, x_2, \dots, x_n) = c_{g_0}(x_2, \dots, x_n) =$$
$$= c_{f_{-d_1}}(x_2 - d_2, \dots, x_n - d_n) = c_{f_{-d_1}}^{\delta'}(x_2, \dots, x_n);$$

$$c_f^\delta(j, x_2, \dots, x_n) = c_g(j, x_2, \dots, x_n) = -\sum_{i=1}^{k-1} i^{k-1-j} c_{g_i}(x_2, \dots, x_n) =$$
$$= -\sum_{i=1}^{k-1} i^{k-1-j} c_{f_{i-d_1}}(x_2 - d_1, \dots, x_n - d_n) =$$
$$= -\sum_{i=1}^{k-1} i^{k-1-j} c_{f_{i-d_1}}^{\delta'}(x_2, \dots, x_n), \quad j = 1, \dots, k-2;$$

$$c_f^\delta(k-1,x_2,\dots,x_n) = c_g(k-1,x_2,\dots,x_n) = -\sum_{i=0}^{k-1} c_{g_i}(x_2,\dots,x_n) =$$

$$= -\sum_{i=0}^{k-1} c_{f_{i-d_1}}(x_2-d_2,\dots,x_n-d_n) = -\sum_{i=0}^{k-1} c^{\delta'}_{f_{i-d_1}}(x_2,\dots,x_n).$$

Теорема 1 доказана. □

В соответствии с доказанными в теореме 1 свойствами для функции $f(x_1,\dots,x_n)$ вектор коэффициентов ее поляризованного по вектору δ полинома $\tilde{c}_f^\delta$ может быть рекурсивно найден по вектору ее значений $\tilde{f}$. Несложно подсчитать, что при этом будет затрачено $O(N\log N)$ битовых операций, где $N=k^n$ – длина векторов.

Известна формула подсчета значений коэффициентов обычных полиномов булевых функций по их значениям [5]: если $f(x_1,\dots,x_n)\in P_2^n$, то для каждого набора $\alpha=(a_1,\dots,a_n)\in E_2^n$ верно

$$c_f(\alpha) = \sum_{\beta:\beta\preceq\alpha} f(b_1,\dots,b_n),$$

где $\beta=(b_1,\dots,b_n)\in E_2^n$.

В следующей теореме 2 мы предлагаем формулы подсчета коэффициентов поляризованных полиномов k-значных функций по их значениям.

Сначала введем несколько определений. Для набора $\alpha=(a_1,\dots,a_n)\in E_k^n$ обозначим как $I(\alpha)$ множество индексов его ненулевых координат,

$$I(\alpha)=\{i : a_i\neq 0\}.$$

Число ненулевых координат набора α назовем его *весом* и обозначим $|\alpha|$,

$$|\alpha| = |I(\alpha)|.$$

Теорема 2. *Пусть k – простое число, $f(x_1,\dots,x_n)\in P_k^n$, $\delta=(d_1,\dots,d_n)\in E_k^n$ – вектор поляризации.*

Тогда для каждого набора $\alpha=(a_1,\dots,a_n)\in E_k^n$ верно равенство

$$c_f^\delta(\alpha) = (-1)^{|\alpha|}\sum_{\beta:I(\beta)\subseteq I(\alpha)}\left(\prod_{a_i\neq 0} b_i^{k-1-a_i}\right) f(b_1-d_1,\dots,b_n-d_n),$$

где $\beta=(b_1,\dots,b_n)\in E_k^n$ (полагаем, что произведение $\prod$ по пустому множеству индексов равно 1 и $0^0=1$).

Доказательство. 1. Вначале рассмотрим обычные полиномы, то есть предположим, что вектор поляризации $\delta=(0,\dots,0)$.

Для этого случая доказательство проведем индукцией по числу переменных функции n.

Базис индукции: $n=1$. Тогда для набора $\alpha=(a_1)\in E_k^1$ по теореме 1 получаем

1) если $a_1=0$, то

$$c_f(a_1) = f(0) = (-1)^{|\alpha|}f(0);$$

2) если $a_1=1,\dots,k-1$, то

$$c_f(a_1) = -\sum_{i=0}^{k-1} i^{k-1-a_1} f(i) = (-1)^{|\alpha|}\sum_{\beta:I(\beta)\subseteq I(\alpha)} b_1^{k-1-a_1} f(b_1).$$

Индуктивный переход. Пусть для всех функций, зависящих не более чем от $n-1$, $n \geq 2$, переменной, утверждение теоремы 2 верно. Рассмотрим функцию $f(x_1, \ldots, x_n) \in P_k^n$.

Пусть $\alpha = (a_1, \ldots, a_n) \in E_k^n$ и $\alpha' = (a_2, \ldots, a_n)$. Тогда по теореме 1 и с учетом индуктивного предположения получаем

1) если $a_1 = 0$, то

$$c_f(0, a_2, \ldots, a_n) = c_{f_0}(a_2, \ldots, a_n) =$$

$$= (-1)^{|\alpha'|} \sum_{\beta' : I(\beta') \subseteq I(\alpha')} \left(\prod_{a_i \neq 0, i \geq 2} b_i^{k-1-a_i} \right) f_0(b_2, \ldots, b_n) =$$

$$= (-1)^{|\alpha|} \sum_{\beta : I(\beta) \subseteq I(0, \alpha')} \left(\prod_{a_i \neq 0} b_i^{k-1-a_i} \right) f(0, b_2, \ldots, b_n),$$

где $\beta = (b_1, b_2, \ldots, b_n) \in E_k^n$ и $\beta' = (b_2, \ldots, b_n)$.

2) если $a_1 \neq 0$, то

$$c_f(a_1, a_2, \ldots, a_n) = -\sum_{b_1=0}^{k-1} b_1^{k-1-a_1} c_{f_{b_1}}(a_2, \ldots, a_n) =$$

$$= -\sum_{b_1=0}^{k-1} b_1^{k-1-a_1} \left((-1)^{|\alpha'|} \sum_{\beta' : I(\beta') \subseteq I(\alpha')} \left(\prod_{a_i \neq 0, i \geq 2} b_i^{k-1-a_i} \right) f_{b_1}(b_2, \ldots, b_n) \right) =$$

$$= (-1)^{|\alpha|} \sum_{\beta : I(\beta) \subseteq I(\alpha)} \left(\prod_{a_i \neq 0} b_i^{k-1-a_i} \right) f(b_1, b_2, \ldots, b_n),$$

где $\beta = (b_1, b_2, \ldots, b_n) \in E_k^n$ и $\beta' = (b_2, \ldots, b_n)$.

2. Теперь рассмотрим произвольный вектор поляризации $\delta = (d_1, \ldots, d_n)$. Воспользуемся тем, что поляризованный по вектору $\delta = (d_1, \ldots, d_n)$ полином функции $f(x_1, \ldots, x_n)$ является обычным полиномом для функции

$$g(x_1, \ldots, x_n) = f(x_1 - d_1, \ldots, x_n - d_n).$$

Тогда для каждого набора $\alpha = (a_1, \ldots, a_n) \in E_k^n$ по доказанному получаем

$$c_f^\delta(\alpha) = c_g(\alpha) =$$

$$= (-1)^{|\alpha|} \sum_{\beta : I(\beta) \subseteq I(\alpha)} \left(\prod_{a_i \neq 0} b_i^{k-1-a_i} \right) g(b_1, \ldots, b_n) =$$

$$= (-1)^{|\alpha|} \sum_{\beta : I(\beta) \subseteq I(\alpha)} \left(\prod_{a_i \neq 0} b_i^{k-1-a_i} \right) f(b_1 - d_1, \ldots, b_n - d_n),$$

где $\beta = (b_1, \ldots, b_n) \in E_k^n$.

Теорема 2 доказана. □

Работа частично поддержана РФФИ (проекты № 07-01-00444 и 09-01-00701-а.)

Summary

S.N. Selezneva, N.K. Markelov. Fast Algorithm for Building Polarized Polynomial Coefficients' Vectors of k-valued Functions.

The fast algorithm for building the polarized polynomial coefficients' vectors of k-valued functions by their values is proposed (for prime k). The formulas for polarized polynomial coefficients of k-valued functions by their values are obtained.

Key words: k-valued function, polarized polynomial, fast algorithm.

Литература

1. *Яблонский С.В.* Введение в дискретную математику. – М.: М.: Высш. шк., 2001. – 384 с.
2. *Селезнева С.Н.* О сложности представления функций многозначных логик поляризованными полиномами // Дискр. матем. – 2001. – Т. 14, Вып. 2. – С. 48–53.
3. *Гаврилов Г.П., Сапоженко А.А.* Задачи и упражнения по дискретной математике. – М.: Физматлит, 2004. – 416 с.
4. *Супрун В.П.* Табличный метод полиномиального разложения булевых функций // Кибернетика. – 1987. – № 1. – С. 116–117.
5. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 469 с.

Поступила в редакцию
24.04.09

Селезнева Светлана Николаевна – кандидат физико-математических наук, доцент кафедры математической кибернетики факультета ВМК Московского государственного университета им. М.В. Ломоносова.

E-mail: *selezn@cs.msu.su*

Маркелов Николай Константинович – студент кафедры математической кибернетики факультета ВМК Московского государственного университета им. М.В. Ломоносова.

E-mail: *nord_rk@bk.ru*